AC/323-D(2002)36
4 April 2002

North Atlantic Treaty Organization
Research and Technology Organization

RTO Combating Terrorism Workshop Report

20020613 200

Held on 5-7 February 2002
In Arlington, VA, USA

This page intentionally left blank

Executive Summary

In February 2002, the NATO Research and Technology Organization held a Combating Terrorism (CT) Workshop in Washington, D.C. The goals of the workshop were:

- To develop a list of high impact R&T areas that the RTO and other NATO organizations could sponsor as part of NATO's overall effort to combat terrorism.
- To foster a multi-national exchange of ideas that will enhance both national and multinational R&T activities for combating terrorism.

To achieve these goals, the RTB Chairman and RTA Director, in concert with the RTO Panel Chairs, arranged for four or five members of each of the RTO technical panels and group to be brought together, along with representatives from other NATO and national bodies, to examine how technology might contribute to combating terrorism. The participants were placed in one of four facilitated workgroups to discuss approaches to this issue based on generic attack scenarios. Conclusions and ideas were then presented in a plenary session of all participants, and then finalized. Given that the work of the experts was conducted over only a bit longer than one day, a large volume of topics was not expected. Given that the participants represented a wide technical spectrum and many nations, it was expected that the ideas would be worthwhile, and could well be unique.

In order to insure that the participants in the workshop would be better able to contribute, they were provided with information and views which would set the context for combating terrorism, which would provide both national and international views and concerns, and which would describe the challenges of the combat as seen by those who have been deeply engaged.

The workshop produced ideas for technologies and technological issues that need to be addressed in combating terrorism. The areas of proposed cooperation and the titles of the particular topics are listed here in summary form:

1. Sensors & Biometrics

    - AUV's with Sensor Suites
    - Sensors for Vapor, Dust, People Inside Vehicles, and Enclosed Compartments
    - Improved Stand-Off Bio-Detection
    - Warning System Around High-Value Systems
    - Underground Surveillance of Tunnels, Sewers and Parking Lots
    - Means to Differentiate Terrorists from Civilians
    - Explosives Detection with Stand-Off Ranges
    - Biometrics
    - Access Control
    - Using Existing Infrastructure for Distributed Sensors and Communications
    - Defence in Depth
    - Dispatch Control of Delivery Vehicle
    - Unattended Sensors for Reconnaissance Down to Individual Level

2. Database Technologies

- Access to Databases
- Evaluation of Data Search Tools
- Database on Terrorist Activity/Characteristics
- NATO Information Architecture for Rapid Warning and Attribution Analysis
- Tools for the Common Information Picture
- Early Identification and Spotting of Disease
- Defining Baselines for Essential Science/ RTO Panel Cooperation
- Review of Existing Databases and Reusable Models
- Networking, Analysis and Trigger Algorithms
- Real time Scenario Construction of Terrorist Operations
- Control of Purchase of Material

3. Cyber Security/Protection

- Inforensics
- Real Time Net Intrusion Detection
- Distributed Denial of Service Attacks
- Mobile Ad-Hoc Networks
- Surrogate Targets
- Malicious Software
- Wrapper Technology
- "Out of the Box" Technologies

4 Decision Support/Command and Control

- Adapting Existing Military Command & Control to Terrorism Response
- Risk Communication and Management

5. Modelling and Simulation

- CT Performance and Assessment Models
- Modelling and Simulation
- Urban Dispersion Modelling
- Epidemiological Modelling

6. Biological

- Cooperation on Decontamination Technology
- Medical Treatment Modalities for Consequence Management of CBRN Events

7. Access Control

- Stricter Control of Small Aircraft

8. Training

   - Novel Techniques and Technologies for Training First Responders and Higher Echelons

9. Material Tagging

   - Tagging

10. Weapons

    - Novel Energetic Materials
    - Special Payloads to Defeat CBRN Threats with Minimum Collateral Damage

11. Physical Protection

    - Personal Protective Equipment
    - Hardening Constructions
    - Shock Wave Mitigation Devices
    - Evacuation Aid

These idea's are detailed in the body of the report. Further collaboration and development into R&T projects or studies will take place through three avenues:

- The report will be distributed throughout the nations of the Alliance. They are expected to distribute it within their R&T communities for consideration by national experts as to whether the ideas and suggestions are suitable for the definition of a national program, based on one or more of them. A related benefit of the workshop is that national representatives who participated are expected to carry home with them the ideas that were discussed (even those that were not documented fully) and to expand these ideas in a national context.

- The report will be distributed to each of the panels of the RTO and to the NMSG. These bodies are charged with considering the issues and studies recommended in it and to define how they might contribute to them, either individually as panels or jointly. They will be asked to report back to the RTB on their conclusions and recommended way ahead.

- As the report is reviewed by national experts, it is expected that additional suggestions for areas of study will come to light. The RTO would like to encourage continued dialogue and requests that comments and recommendations be forwarded to the RTA through respective National Coordinators.

This page intentionally left blank

TABLE OF CONTENTS

1. INTRODUCTION[1]

1.1. The goals of the NATO RTO Combating Terrorism (CT) Workshop were:

- To develop a list of high impact R&T areas that the RTO can sponsor as part of NATO's overall effort to combat terrorism.
- To foster a multi-national exchange of ideas that will enhance both national and multinational R&T activities for combating terrorism.

1.2. To achieve these goals, the RTO arranged for four or five members of each of the RTO technical panels and group to be brought together, along with representatives from other NATO and national bodies, to examine how technology might contribute to combating terrorism. The participants were placed in one of four facilitated workgroups to discuss approaches to this issue based on generic attack scenarios. Conclusions and ideas were then presented in a plenary session of all participants, and then finalized. Given that the work of the experts was conducted over only a bit longer than one day, a large volume of topics was not expected. Given that the participants represented a wide technical spectrum and many nations, it was expected that the ideas would be worthwhile, and could well be unique.

1.3. In order to insure that the participants in the workshop would be better able to contribute, they were provided with information and views which would set the context for combating terrorism, which would provide both national and international views and concerns, and which would describe the challenges of the combat as seen by those who have been deeply engaged.

1.4. The workshop produced ideas for technologies and technological issues that need to be addressed in combating terrorism. The contents and conclusions are listed in the body of this report. They are necessarily of a very summary nature and must be examined carefully and expanded in detail. This is the task of experts in nations and within NATO. The proposals for further effort are presented for the use of all readers, not just for the RTO. The suggestions should be considered within the nations and by other bodies and agencies of NATO. Within the RTO, the Panels should consider how the concepts could be explored, either by a single panel or by several panels working together.

[1] Director's Acknowledgements:
The Director of the RTA would like to acknowledge the significant support which the RTO received from a number of people and agencies is putting this workshop together. The U.S. DoD, in the offices of DDR&E, AFOSR and SAF/AQR provided outstanding support with staff and facilities. Two U.S. co-organisers, Mr. Alan Murashige and Dr. Yolanda Jones-King, were instrumental in working the concept and the details. At the RTA, LtCol Weisz contributed indispensibly to the preparations as well as the completion of the report.

2. CONSTRAINTS/ASSUMPTIONS

2.1. In structuring the CT workshop, there were several constraints that needed to be acknowledged. These constraints are outlined here.

2.1.1. As with all R&D, there should be a balance between requirements pull and technology push. In the domain of CT, particularly in the NATO context, the statement of requirements is not easily obtained. There is no formal NATO requirement statement at this time. In the national context the situation is similar, for those who are concerned with the issues are often not able to articulate their needs beyond the most general type. This was not a hindrance to the technology specialists who were present; they were able to define scenarios and from these derive the technology requirements.

2.1.2. Further to the lack of clearly defined military requirements, the political context is evolving slowly. National views on positions for combating terrorism are being defined and while the collective NATO position is defined by the invocation of Article 5, the implications of this declaration have yet to be defined.

2.1.3. There are a host of non-technical factors that are of great importance in combating terrorism. These include sociological considerations, economic status, infrastructure vulnerabilities and strengths, psychological effects, intergovernmental coordination issues, and the like. Non-technical factors derived from the workshop are included in the Workgroup Results section.

2.1.4. While those participating in the workshop were experts from the world of defence R&T, defence is not the only principal player in combating terrorism. There are many other departments and agencies involved, such as those which deal with health, transport, policing, mail, intelligence and energy.

2.2. The presence of such constraints did not prove to be a hindrance. The participants recognized them, but felt that their knowledge base was sufficiently wide such that their contributions were able to stand-alone and have sufficient breadth that they could make a significant contribution notwithstanding the constraints.

3. CONTEXT SETTING SUMMARY

3.1. Context Setting Presentations

The workshop's main business, conducted in four concurrent workgroups, was prefaced by a series of authoritative Context Setting presentations involving the entire first day plus portions of other days. Several themes emerged involving:

- Threat – status of analysis and requirements definition
- Catastrophic and asymmetric nature of the threat
- Unique national and alliance challenges and CT problems posed
- Need for a global response and alliance-wide solutions
- Role of technology in creating critical CT capabilities
- Impact of "non-technical" elements in crafting solutions
- Existence of current national views and initiatives based on prior terrorism and CT national activities

A brief summary of context setting presentations (in the order they were presented) follows. Complete titles and affiliation of presenters is included in the agenda (Appendix 1). The text of presentations and/or briefing charts are found in a separate volume of the proceedings.

3.1.1. Intelligence Overview

Lt-Col P. Stack (UK), HQ NATO Intelligence Branch, summarized the status of the evolving threat analysis currently under way for the terrorism and CT areas. Although this analysis is not complete nor formally approved through the NATO intelligence production process, several insights and trends relevant to the workshop are evident. Worldwide terrorist capabilities are impressive and cover a full range of traditional autonomous military activities and information technology operations deliverable through the Internet. Terrorists possess extensive indoctrination and educational capabilities and infrastructure to further their aims. Coupled to specific objectives and initiatives to gain access to weapons of mass destruction further intensifies the long-term threat. Priority concerns to NATO include warhead security and vulnerability to theft of nuclear materials from both military and civilian sources, particularly in countries in the midst of moderate to severe economic or military turmoil. Vulnerabilities and sheer magnitude inherent in worldwide media and information operations pose a daunting challenge. Overall trends in capabilities, threats and the nature of terrorist organizations include:

- Overall sophistication – increasing in scope and complexity
- Chemical/Biological – increasing, especially in ability to conduct larger scale operations; taking on strategic vs. just tactical dimensions
- Weapons of Mass Destruction – significantly increasing ability to deliver via multiple means (air, land, sea)
- Small scale operations – remain the most common employment strategy (notwithstanding the impact of the World Trade Center attack)
- Linkages to drug organizations and organized crime – relatively constant, but an enabling factor especially for financing terrorist activity, infrastructure and training
- Intent – much more ambitious and determined comparing the present time with the past (1960s – late 1980s)

3.1.2. The Nature of the Threat

Maj. Gen. F. E. van Kappen (NL), former Military Advisor to the UN Secretary General, emphasized the importance of comprehending the nature of the still evolving threat. He underscored that this "deadly cocktail" threat is:

- Strategic – it exists and continues to develop worldwide, including in nations which heretofore have not yet experienced terrorism
- Asymmetric – in sharp contrast to conventional warfare with traditionally arrayed forces, rules of engagement and acceptance of international law, all of which are intentionally disregarded by terrorists to gain advantage and achieve unexpected impacts. The very fabric of civilized society is the primary target.
- Apocalyptic – seeking specifically to inflict suffering, death and damage on a grand scale with no regard for short or long term impacts on innocent civilians, including children, and when necessary, on their own members. The same is true for impacts on infrastructure (often targets) or the environment.
- No rules, no negotiation, no restrictions – driven by a deeply rooted belief in the total inferiority of western societal and governmental basic principles, values and norms. An analogy from a western cultural perspective might be that of the Christian concept of the "Devil".
- Not always Islamic – terrorist causes are sometimes embraced, either through sympathy with motivation or by indoctrination/training by non-Islamic individuals, groups or, conceivably, nations.
- One-sided understanding – reality is that terrorists, as a whole, have invested long-term effort and study to understanding us in sharp contrast to our very limited understanding of them. They have lived with and participated in the features of western society, often for years prior to being called upon to execute an attack. They begin the process of education and training with children and continue the process indefinitely. In terms of understanding the adversary, they have been proactive; we have been mainly reactive. We do not tend as a people to study easily what we do not understand or find offensive.

In coping, NATO is confronted with several challenges beyond the threat, such as those stemming from NATO member-nation accepted differences. Although we now see the physical threat similarly, we may differ on the relative importance of elements, and thus response, to specific threats. This poses challenges to the allies regarding agreement on priorities, allocation of resources and (for purposes of this workshop) which technologies and capabilities to undertake collaboratively. Further, because of the severity and enduring nature of terrorism as we now begin to comprehend it, we are faced with difficult choices such as how much "freedom" to trade for security. The nature of this war will be "dirty" beyond anything we might have known in the past and not of our choosing. In addition to repugnant physical dimensions, it will involve offensive, defensive virtual Net warfare (multiple nodes) and Media warfare on a scale yet to be understood.

3.1.3. Spanish Approach to CT Technology

Mr. A. Relanzon (SP) shared his view of the threat, as Spain has been experiencing and countering for many years. A specific set of neutralization approaches and a representative application case was described. The importance of applying existing technology, developing new technology to augment existing capabilities and the importance of dealing with human factors and limitations was stressed.

3.1.4. Global Aspects of the Terrorist Threat

Prof. Sir Keith O'Nions (UK), Chief Scientific Advisor to the MOD, provided UK insights on the global nature of terrorist threats calling for global solutions, such as those that might be generated by an enduring NATO collaborative technology initiative. He underscored that the response must be long-term and not just a series of activities for the purpose of showing numbers of admittedly sound activities. Many inhibitors to effective threat mitigation will be present because of the diffuse nature of the threat and the many dimensions the adversary can trigger. NATO's technology response must be significant, enduring and support collective evolution of effective capabilities and solutions.

3.1.5. US Technology Response to CT

Dr. R. Sega (US), OSD/DDR&E, provided a description of the nature and purposes of the recent (since September 11) US initiative under the aegis of the US CT Technology Task Force (CTTTF). His all agency task force focuses on a full range of CT technology possibilities to establish capabilities that could be brought to bear by CT forces within 30 days, 1 year and up to 5 years nominally. Proposals are being solicited through a massive Broad Agency Announcement (BAA) and have stimulated over 12,000 conceptual responses, including 85 from abroad (many from NATO nations). It is anticipated that these inputs, once reduced to several hundred of the most promising, will be solicited for more detailed proposals with an undetermined number to be funded with new Homeland Defence resources as well as re-prioritized agency funds. A particular effort will be made to consider innovative proposals that will be of value to the NATO implementation of workshop results.

3.1.6. Organizing a National Response

Dr. P. Albright (US), White House Office of Science and Technology Policy, provided a Bush Administration perspective for the US response to recent terrorist attacks. In addition to the military response detailed publicly, the new and combined multi-agency and federal, state and local response was reviewed. This multifaceted approach is unprecedented in modern times, if ever, and poses major questions as to long-term impacts on open communications (including scientific) and the controversial issue of possibly imposing security clearances on selected state and local officials. To begin to manage these and other new issues arising from the CT war, the US has created a new Homeland Defence Agency just beginning now to become operational. A specific purpose is to define and refine interagency CT roles, national CT priorities, and budgets. To assist, a series of interagency crosscutting working groups are being established. The impact on NATO CT technology activities is yet to be determined and should be revisited as the outcome of the workshop and follow-on activities become clear.

3.1.7. Challenges to the Alliance

Mr. M. Markin (UK), Director General, MOD, provided a perspective on the CT problem and unique challenges which demand new national and alliance approaches, many involving non-technical aspects. Mr. Martin suggested that a full range of initiatives must be considered in the organizational, social and psychological arenas. Specifically, the requirement for creating a series of international analysis centers to act upon massive amounts of intelligence data and inter-linked national CT Defence Intelligence Centers and CT Battle Labs (being establishing now) was discussed. The need to consider lethal and non-lethal technology possibilities was emphasized.

The question of establishing such a "Battle Lab" to support RTO initiatives stemming from the workshop was introduced.

3.1.8. Canadian Approach to a National Response

Dr. J. Leggat (CA), CEO Defence R&D, described his national CBRN R&T initiatives built around an integrated approach. A Federal Innovation Center of Excellence has been developed employing virtual "cluster" modelling and simulation capabilities across the federal government. The result is a significantly enhanced national capability and tools to perform CT operational capability, threat gap analysis and impact assessments involving nationwide resources. A workshop on this subject is scheduled for early March and workshop attendees are invited to attend.

3.1.9. The US CT Technical Support Working Group

Mr. E. McCallum (US), Director of Combating Terrorism Technical Support Office (CTTSO), OSD/SOLIC, provided an overview of the US CT Technical support Working Group process referenced earlier by Dr. Sega (US). In addition to the process, described in detail in the proceedings, Mr. McCallum stressed that technologies for stand-off detection of terrorist threats and activities is a new priority for US CT and may well be for NATO as well.

3.1.10. DARPA Technologies for CT

Dr. J. Alexander (US), Deputy Director, Defense Advanced Research Projects Agency (DARPA), provided a summary, with extensive examples, of specific DARPA CT technology projects. These are documented for reference in the proceedings.

3.1.11. Analytical Framework for Integrated Approach to CT

Dr. G. Barbarosoglu (TK), Director, CENDIM Center for Disaster Management, provided an analytical framework for an integrated approach to combating terrorism. The approach is based upon the long experience Turkey has in dealing with earthquake catastrophes but applied to terrorism as a disaster event. From this experience and extrapolation, a set of general principles for guiding international cooperation on CT was offered. These include: identification of an agreed-to common set of CT relevant definitions (taxonomy); identification of areas of intended international cooperation and any coalitions that need to be built; formation of an international working group to implement solutions; determination of actions, including sanctions, to be imposed for effective CT; and the identification of a generic framework for pursuing CT solutions. Within these principles, specific actions were proposed for NATO consideration, including: proposed changes to the workshop base line taxonomy involving placement and/or definition of crisis management, threat warning, and incident management; proposed process analysis of CT functions; generation of a fully integrated CT taxonomy; identification of a CT Technology Support structure; definition of a methodology (3-phase approach) for developing a decision support capability for CT; and definition of a "conceptual architecture" for defining NATO CT organizations, processes and initiatives.

3.1.12. RTO CT Program

Mr. K. Peebles (CA), Director, RTA, summarized the RTO CT program and NATO HQ views on CT. Key on-going activities of interest to the workshop and serving as a partial point of departure include: multiple scenario threat definition; protection methods and technologies from NBC sources; human factors (including physiological and psychological aspects); information operations (protection and attack); vehicular technologies (structures, propulsion, including aircraft, ships, land vehicles); overall system vulnerability (weapon systems, information systems and infrastructure); detection capabilities and technologies (multi-platform); and modelling/simulation capabilities to support operations, analysis and technology development. The extensive current RTO program and panels/group should provide a valuable source of collaboration source technology and talent to support CT focused future endeavors.

3.1.13. The US Position in CT

Ambassador F. Taylor (US), State Department Coordinator for CT, provided a US CT status briefing recently given to the North Atlantic Council (this briefing is not available for dissemination). A key point made relative to the challenge confronting the workshop is that the terrorism threat, in sharp contrast to all recent threats, demands a coordinated response from all military, economic, financial, intelligence and law enforcement agencies and institutions – simultaneously and world-wide indefinitely. Underpinning the achievement of this level of response will be an unprecedented need for integrated multinational, databases & information sharing & knowledge management, applicable to all phases of CT warfare.

3.2. Poster Session – An Introduction to Relevant R&D Projects Already in Work

An unclassified, multi-national "Poster Session" consisting of 31 illustrated CT technology display boards (each with an expert spokesperson) was made available to attendees during the workshop. A broad range of technologies directly or potentially applicable to improved CT capabilities was represented. Major technology themes included a variety of C4ISR, detection, imaging, training and bio/genetic methodologies applicable across the full range of required CT response missions. Workshop members were asked to make a special effort to visit posters in their areas of interest and bring these technologies back into the workgroup deliberations as possible elements of future NATO collaboration.

4. WORKGROUP DEFINITIONS

Four workgroups were designed to cover the full spectrum of combating terrorism. Participants in the respective workgroups focused on their assigned area based on the following workgroup definitions:

4.1. INDICATIONS & WARNING:

Improved terrorist and agent identification, surveillance and tracking capabilities to help prevent terrorist acts by facilitating the timely interdiction of terrorists and threat agents and devices, and the identification of emerging terrorist threats at an early stage. Early warning of impending attack to enable the implementation of protective countermeasures.

4.2. SURVIVABILITY & DENIAL:

Denying access to potential targets is a critical aspect of preventing terrorist attacks. Effective means for limiting access to facilities, combined with advanced threat detection and screening capabilities will inhibit many actions by terrorists by preventing them from reaching intended targets.

4.3. CONSEQUENCE MANAGEMENT & RECOVERY:

Measures to protect public health and safety, restore essential government services, and provide emergency relief to governments, businesses and individuals affected by the consequences of terrorism.

4.4. ATTRIBUTION AND COUNTER-ACTION:

The development of improved capabilities for rapidly and reliably identifying the perpetrators of terrorist incidents will enable the planning and execution of appropriate counter-action operations as well as the implementation of effective countermeasures to possible additional attacks. Improved forensic capabilities will also support criminal prosecution efforts by the appropriate governmental entities in each country. The ability to execute a variety of military operations in response to terrorist attacks is important for deterring future incidents. New capabilities for conducting such operations with greater speed, precision and a higher level of assured effectiveness are needed to reduce casualties suffered by national/coalition forces and to minimize fratricide problems, particularly in hostage situations.

5. REPRESENTATIVE CT SCENARIOS/CAPABILITIES

Each workgroup defined a set of scenarios and desired capabilities (as described below) to base their technology proposals on. The scenarios and desired capabilities were defined by the participants solely for the purpose of developing ideas, and are not based on official NATO or national positions.

5.1. INDICATIONS & WARNING WORKGROUP

This group focused on short-term warning and long-term indication needs based upon a broad range of terrorist incidents and delivery means (human, animal, platforms - ships, planes, vehicles, etc.). The desired capability was to detect and analyze events or features within available data sources to provide indicators and alarms. The desired longer-term capability is to detect and monitor potentially threatening terrorist action with a desire to maximize standoff range and area coverage of sensors.

5.2. SURVIVABILITY & DENIAL WORKGROUP

This group defined 4 terrorist attack scenarios:

- Attack on a highly populated point target with explosives;
- Cyber attack on critical infrastructure;
- Wide area biological attack on human vital components;
- Sequential attack involving the previous 3.

5.3. CONSEQUENCE MANAGEMENT & RECOVERY WORKGROUP

This group defined 2 scenarios:

- A radioactive attack against a key node (either military or civilian). The desired capability for this scenario was to return to normal operations as soon as possible.
- A medical "pandemic" (catastrophe) with effects across people and animals, based on use of poxvirus, Ebola, HIV, plague, and a designer/novel virus. This scenario focused on 6 smallpox-contaminated terrorists boarding an airliner (200 passengers) bound for a major city airport in a NATO country. They defined smallpox as a worse case and that the underlying process is applicable to other contagious diseases. The desired capability, needs, or requirements were:
  - Early detection of the risk and trigger
  - Diagnosis of smallpox
  - Training for doctors, teachers, health workers and other relevant personnel
  - Improve awareness of the disease and its risk
  - Treatment and vaccination
  - Containment
  - Disposal

5.4. ATTRIBUTION AND COUNTER-ACTION WORKGROUP

Based on multiple scenarios, this group defined 7 broad desired capabilities:

- Attribution Capabilities: analysis, real time scenario construction, cooperative integration of military and civilian organizations, forensics, timely ID of sources of cyber attack
- Counter-action Capabilities: coping with multiple complex scenarios/threats, coping with individual threats

6. POSSIBLE AREAS OF COLLABORATION:

The workgroups produced a multitude of ideas for technologies and technological issues that need to be addressed in combating terrorism. The proposals come from the participants, not from established NATO or national needs. The ideas have been re-grouped based on broad categories of similar items. This list is provided for use by R&T experts within an RTO panel or individually within nations.

6.1. SENSORS & BIOMETRICS

6.1.1. Autonomous Underwater Vehicles (AUV's) with Sensor Suites

Description: There are many technological problems associated with tracking shipping, detecting devices and clearing sea mines. Many of these require a rugged, sea-going capability for sensing and communicating threats both above and below the surface.

Purpose: AUV's promise to provide platforms for sensors that can survey, detect and classify, then transmit to a command center, anomalous objects (weapons, swimmers, etc) in ports or on ships, as well as provide clandestine capabilities to monitor communications to augment human intelligence in near-shore areas.

6.1.2. Sensors for Vapor, Dust, People Inside Vehicles, and Enclosed Compartments

Description: Technologies for sensing standoff and in-situ minute quantities of vapors indicative of common explosives are in development. This includes polymers optimized to respond when pumped by light-emitting diodes to fluoresce in the presence of key vapor components and mass spectrometry techniques. Human presence in enclosed areas such as shipping containers and hidden in vehicles can be detected via laser vibrometry and handheld radar techniques at moderate standoff distances. The laser vibrometry phenomenology is based on the inherent vibration/acoustical signature resulting from breathing/heartbeat, while the radar techniques are sensitive to gross human presence or movement.

Purpose: Studies in the following domains need to be considered:

- Lidar fluorescence, absorption or transmission
- Lidar back-scattering
- Spectroscopy
- Micro-spectral analyzers on a chip
- Materials which react to the threat

6.1.3. Improved Stand-Off Bio-Detection

Description: It is difficult to detect pathogenic bio-agents early and reliably in-situ, including in air, food, water, blood, body, etc., and even more difficult to detect bio-agents remotely and without contact.

Purpose: To determine possible improvements in currently available techniques. To develop cheaper mobile systems that can operate autonomously. To develop improvements in specificity, while being able to cover a wide range of agents.

6.1.4. Warning System Around High-Value Systems

Description: Short and long range surveillance systems to be deployed on and around high value targets. These include radio frequency, millimeter-wave or laser radars, acoustic or seismic sensors, passive optical, infrared or radio-wave sensors.

Purpose: The output from a set of the above sensors could be fused together to increase the probability of detection and identification of the threat. The information provided by the sensors, either raw or processed, would be fed to proper command and control information systems for appropriate follow-up actions.

6.1.5. Underground Surveillance of Tunnels, Sewers and Parking Lots

Description: Parking lots are conducive to more extensive non-intrusive search because the vehicle is stationary for an extended period of time. These areas are easier to deal with than high traffic areas because of the time factor. One could declare exclusive zones, e.g. sewers, and report all entries, and use optical/infra-red camera, movement detector, chem./bio-detector, and autonomous ground vehicles with sensors.

Purpose: Studies in the following domains need to be conducted:

- Passive optical (visible, infrared)
- Active optical (laser, active imaging)
- Acoustic / seismic
- X-Rays
- Electromagnetic resonance (dipole)
- Data fusion of various sensors

6.1.6. Means to Differentiate Terrorists from Civilians

Description: Conducting counter-terrorism operations requires reliable methods for identifying potential terrorists in a civilian environment. This will require tools to differentiate on the basis of behavioral and other characteristics.

Purpose: The work program will:

- Define a basis for discriminating and identification
- Develop protocols for signature profiling and observation
- Investigate applicable technologies for sensing and interpretation.

6.1.7. Explosives Detection with Stand-Off Ranges

Description:
There is a need for a catalogue of portable prototype and fielded devices for explosives materiel detection at stand-off ranges of x (TBD) meters for use by security personnel in urban and remote locations..

Purpose: Conduct a market survey and create the needed catalogue.

6.1.8. Biometrics

Description: Biometrics includes a number of areas (voice recognition, voice identification, fingerprints recognition and facial recognition) that are being researched within NATO countries. Results obtained up to this moment are partially positive. For example, one can recognize a specific person, but it is still difficult to do this when the person is in a crowd. Expectations for the near future are promising.

Purpose: A concerted effort should be conducted to improve the cooperation in Biometrics especially between NATO experts and Academia, because academic institutions perform most of these activities.

6.1.9. Access Control

Description: There are a variety of available technologies available to include fingerprint recognition and face recognition. These are typically used to admit individuals that are input into the database. They can be used to exclude certain individuals while admitting all others; however, the issue is speed. In neither case can they be used to admit large populations such as a football stadium. The technology issue is to achieve exclusion of a small population from a large population at a speed commensurate with the proverbial football stadium. Face recognition is the most desirable, as it is most passive. Vehicle license plate reading is practical at ticket taking speeds but not highway speeds. Explosive sniffers are effective at ticket taking speeds.

Purpose: To undertake a study of ways in which existing access control technologies can be used for control in scenarios which can be defined as terrorism related. To further define means by which technology can be improved or introduced to provide further security.

6.1.10. Using Existing Infrastructure for Distributed Sensors and Communications

Description: Possibilities exist to use existing infrastructure within its own domain to provide additional information on status and stability and also to detect intrusions and/or attacks. Another possibility is to use an existing infrastructure to provide a distributed sensor net for a different application domain. For example, installation of bio- or chemical sensors on streetlights, or using ATM machines to profile customers for exposure to bio- or chemical agents or explosives.

Purpose: To perform a study in collaboration with the SAS/SET/SCI Panels and NMSG.

6.1.11. Defence in Depth

Description: Information security is not guaranteed by a firewall. Penetrations still can be achieved through password theft, record theft, malicious elements hidden in a COTS package, etc. Better training and procedures are needed, particularly in the civil infrastructure. Another concern is access control – where biometrics could play a role in achieving positive identification for access to physical and cyber areas.

Purpose: Programs and tasks need to be defined to address the range of topics included in this area. RTO Panel involvement should include HFM, SCI and SAS, with NMSG contributing to system modelling.

6.1.12. Dispatch Control of Delivery Vehicle

Description: It is critical to be able to track deviations from the itineraries of ground vehicles engaged in the transport of dangerous substances which, if diverted, could pose a risk of terrorist activity.

Purpose: Deviations could be sensed against planned itineraries through GPS-based automatic reports via satellite communications links and other appropriate networks. These deviations could then be validated and, if found to be questionable, appropriate authorities can be notified of a potential concern with updates on the location of the vehicle. This would require legal mandates to be implemented.

6.1.13. Unattended Sensors for Reconnaissance Down to Individual Level

Description: Use of cost-effective durable sensors in single or networked functions for providing situational awareness in combating terrorism should be investigated.

Purpose: Research should focus on autonomous functions for alarm, processing and health/status. Power conservation may be achieved by enabling a "sleep" option when the sensor is not required. It is anticipated that these sensors would not be just ground sensors and that various delivery systems (from humans to UAVs to launches) could be used to place them in an area not easily accessed by NATO military forces. These sensors should be persistent (durable, low maintenance, low power consumption, long-life, etc.) and pervasive (many small, almost invisible sensors).

6.2. DATABASE TECHNOLOGIES

Many of the areas for cooperation in this section are proposed because, while there seems to be an infinite amount of data in the modern world, much of this information is stove-piped. Databases are not linked and cannot inter-operate. The organization and structure of one database needs to be known to the others. The proposals below address these issues and their consequences.

6.2.1. Access to Databases

Description: By sharing and analyzing data from different organizations (e.g. police immigration, military), and similar organizations in different nations, it should be possible to determine characteristic features of terrorist organizations and their activities, in both personnel and groups.

Purpose: The proposal is to define candidate database sources, and linking and sharing mechanisms. These cover extended mark-up languages, similar to ADAP-P3 standardized interchange formats, ways of handling different languages updates, etc. This includes both accesses to one database, and linking many databases. The soliciting of database sources should consider other multi-national organizations such as Europol.

6.2.2. Evaluation of Data Search Tools

Description: Evaluate investigative tools for detecting terrorist indicators in large databases.

Purpose: To search for "significant relationships" between features within a set of databases. A variety of data search techniques should be investigated. Key sources for such tools are the COTS marketplace, several key universities and research establishments, and existing work in the RTO IST Panel on data fusion.

6.2.3. Database on Terrorist Activity/Characteristics

Description: To seek characteristics of terrorist activity in a large data set requires "profiles" that characterize such activity.

Purpose: This database should be based on the knowledge of social or behavioral anomalies, but also specific details of known terrorist activity. This database activity would be multi-disciplinary, and include psychological profiling, and other "soft-science" features as well as more explicit features.

6.2.4. NATO Information Architecture for Rapid Warning and Attribution Analysis

Description: The tools to extract, correlate, fuse and exploit data in a timely manner will be developed recognizing proprietary rights and security levels.

Purpose: The purpose of the study is to design an architecture for assembling and processing information that facilitates the identification of perpetrators and supporters. It requires access to diverse and distributed data bases maintained by various military and civilian organizations. It is necessary to identify data needs, databases and data sources and to characterize interoperability and communication architecture.

6.2.5. Tools for the Common Information Picture

Description: This is analogous to the Common Operating Picture (COP) in other domains.

Purpose: A great deal of work would have to be done to design and create an info-sphere COP. Maps of the critical infrastructure would need to be created, links established to pass the data, and methods to detect and establish status must be developed. This would include a strong component of Information Fusion and Visualization, as well as Systems Analysis. Need to link with the HFM/SAS/SCI Panels and the NMSG for exercising the design model. Strong client input would be needed to establish the requirements and usability.

6.2.6. Early Identification and Spotting of Disease

Description: Educate first-line medical professionals, e.g., doctors, pharmacists, nurses on early identification and spotting of diseases.

Purpose: To develop rapid detection of emerging epidemics through the monitoring of unusual trends, e.g., sudden increase of flu-like illnesses from physicians, widespread and increased use of medications associated with specific symptoms and ailments.

6.2.7. Defining Baselines for Essential Science/ RTO Panel Cooperation

Description: Consequence Management requires use of a broad set of techniques and technologies that are horizontally integrated with indications, warning, survivability, and attribution capabilities. (SAS Panel)

Purpose: There is a need for each RTO Panel to understand the science baseline (existent programs & technologies) for each capability essential for Consequence Management. This baseline and a matrix of Panel contributions (i.e., a 2-D matrix of Panel vs. capability) should be developed as a starting point for inter-panel cooperation. Here we need to have a look at who is doing what in the nations to avoid the possibility of duplicating effort. The SAS Panel would examine opportunities for synergies and new collaborative R&D activity, and would need to address the highest priority capability gap areas.

6.2.8. Review of Existing Databases and Reusable Models

Description: Presumably there are many databases and models in use by the nations in both the military and civil sectors. The challenge here is to be able to assess the quality and applicability of the models and databases. Some will be appropriate to the modelling of the critical networks and others will not. The compatibility of models and databases is an important aspect. It would be useful to have a common set of standards for both, but at this time this is not practical. We will need to use interface techniques that are becoming more and more universal as the need to share data drives the technology. In the longer term specific standard approaches such as HLA (High Level Architecture- a simulation standard) will make the job of reuse easier.

Purpose: HFM would undertake an analysis of the Consequence Management capabilities desired to identify which of the capabilities require some underlying model and validated database(s). The Panel would then evaluate the current state-of-the-model/database to determine if they are sufficiently robust for Consequence Management and, if not, propose cooperative exchanges/research to fill the gaps.

6.2.9. Networking, Analysis and Trigger Algorithms

Description: Adaptation of shared working environments (integrated data environments) technologies in an internationally distributed manner to network data information and knowledge from nodes such as: medical units, hospitals, pharmacies, veterinarian offices, medical doctors, pharmaceutical suppliers, etc.

Purpose: Analysis and fusion of these data into knowledge that can be utilized by decision-makers to trigger an alert to initiate diagnosis of smallpox type diseases. A trigger algorithm will be required such that it alerts significant changes from the norm in symptoms, supplies in medication, and medical attention both for humans and animals. Algorithms will have to be validated and tested, and training provided for stakeholders through the use of synthetic environment and modelling and simulation. The networks can also be used during the consequence management phase.
Research / initiative in this domain has to be closely linked to what is in progress (or will be) as part of the WHO (World Health Organization) activities. For example: WHO has different data-

collecting and data-mining tools that are already faster than the tools available in some countries' national health systems.

Some of this is going on already in nations. It is all in the civil sector, being led by health authorities at either the national or state/provincial levels. Military science can contribute by bringing to bear our vast experience in networks, sensors, data fusion, and signal processing. The limitation is the rate at which practitioners feed data into the system. Web-based techniques that allow data input from several sectors of society may reduce reaction time.

6.2.10. Real Time Scenario Construction of Terrorist Operations

Description: Tools for real time scenario construction of terrorist operations should include modelling and simulation, synthetic environments and human behavioral representation.

Purpose: The purpose of this study is to identify the tools needed to provide situational awareness of ongoing terrorist operations in real time. This capability should assist in determining the nature of terrorist acts and the identity of the perpetrators. The information should enable security measures to be rapidly taken to counter any potential follow-on terrorist attacks.

6.2.11. Control the Purchase of Material

Description: Tools are needed to control the purchase of sensitive materials.

Purpose: To identify any means that could be used to identify the buyers of sensitive materials such as explosives, thus confirming the legitimacy of their purchase or denying access of the controlled material. Computerized registration of the purchase of controlled (sensitive) materials is an example of the approach. Computerized records can be analyzed to identify patterns, trends, and thus potentially identify illicit users.

6.3. CYBER SECURITY / PROTECTION

6.3.1. Inforensics

Description: Inforensics is the ability to use forensic techniques to analyze computing equipment for clues, on a computer system after it has been attacked, to establish who has attacked it, where they came from (on the net) and the pattern of attack.

There are two important aspects to Inforensics: examination of seized computers and analysis for evidence; and backtracking and attack characterization to aid in finding perpetrators.

Purpose: To advertise a workshop scheduled this fall and sponsored by IST. Potential for cooperation with SCI/HFM/SAS.

6.3.2. Real Time Net Intrusion Detection

Description: The ability to detect a network intrusion as it happens and record all instances of unauthorized access to networked computers.

Purpose: Given the increased incidence and sophistication of computer network intrusions, to provide real-time warning, thereby avoiding theft of sensitive information, corruption of data and

programs, and/or destruction of control systems (for example, power distribution systems). The IST Panel is sponsoring a symposium 27-29 May 2002 to address this issue.

6.3.3. Distributed Denial of Service Attacks

Description: Distributed Denial of Service Attacks still remain a difficult problem to prevent due to the distributed nature of the threat and the inability of current intrusion detection tools to determine that multiple sources of intrusions are potentially one coordinated, yet distributed, attack.

Purpose: Suggest further IST activity following the current Task Group on Information Assurance, RTG-003, focusing on this specific issue. In particular, a "state of the practice" summary of various commercial and military entities and a "state of the art" research summary would be a valuable starting point.

6.3.4. Mobile Ad-Hoc Networks

Description: Mobile ad-hoc networks are networks that can be quickly set up in a local area (several kilometers in size or greater) to provide radio (wireless digital) communications. Nodes in this network could be on moving vehicles as well as small hand-held devices carried by personnel. With users entering and leaving the network and changing patterns of neighboring nodes, the network must reconfigure itself constantly. Further, these networks differ from more traditional mobile networks in that there is no central server or "hub" in a vehicle or ground control station; each of the units serves both as a node and as a "hop" or link to convey information across the network. This latter activity is complicated by the limited bandwidth of wireless technology, making these disadvantaged grid networks.

Purpose: To study how mobile ad-hoc networks could be used to replace existing communications infrastructure if brought down by physical or cyber attack, or disaster and to study how to better utilize these networks in operational scenarios, either alliance or coalition. Also to study how best to form a communication network of small sensors that can be distributed post-disaster in an area to detect CBRN presence and avoid risk to human life.

6.3.5. Surrogate Targets

Description: Surrogate Targets are lures that are meant to attract hackers/intruders away from the main network. "Fish bowls" allow observation of the intruder by network managers; and, "honey pots" have attractive, but expendable, things in them.

Purpose: To study how surrogate targets could be used to protect NATO networks.

6.3.6. Malicious Software

Description: Otherwise innocent looking COTS software that has malicious code imbedded. The code could be simple viruses, or worms able to perform undesired functions on your computer, such as "sniffing" passwords and sending them to another person by e-mail, or deleting files, etc.

Purpose: To study how to protect NATO networks from this malicious software.

6.3.7. Wrapper Technology

Description: It is a mechanism to encapsulate commercial-off-the-shelf (COTS) software in such a way that it can only execute certain functions. This lowers the risk that the COTS software can execute either intentional (malicious) or unintentional undesired functions.

Purpose: To study how to implement this wrapper technology.

6.3.8. "Out Of The Box" Technologies

Description: The following "out of the box" technologies need to be explored further:

- Using the infrastructure itself as embedded communications or sensing means - e.g. pipelines as communications/sensing medium
- Using old/low technology as a backup
- Low bandwidth, high assurance communications backup
- Practice manual processes, e.g. banks in gyms during '98 Ice Storm in Canada
- Backups - geographical and media diversity for survivable backups
- Remote biometrics
- Non-cyber means of countering cyber attack (police, policies, international law, physical security)
- First responder teams trained in reconstitution of critical networks
- Clusters of Subject Matter Experts (government, industry)

Purpose: To study how to implement these "out of the box" technologies.

6.4. DECISION SUPPORT / COMMAND & CONTROL

6.4.1. Adapting Existing Military Command & Control to Terrorism Response

Description: Command & Control capabilities are important assets in military matters. In the combat against terrorism, important, and often leading roles are played by non-military organizations such as police, fire control, etc. These non-military agencies have their own communication systems, command structures, etc. Interoperability of these systems is essential in successfully countering the effects of terrorist attacks. Inventories should be made of the communication and command structures in place (in particular outside of the defence communities), compatibility determined and, if necessary, action initiated to ensure inter operability as soon as possible. Enabling interoperability between military and civil command systems will require an approach that provides interfaces rather than a common approach. Re-equipping the civil authorities will prove to be too expensive. (IST Panel and NC3A)

Purpose: To examine existing military and civil activity. It should be a joint panel activity; SCI and IST with SCI in the lead. Results of this work should also be examined by NC3A and appropriate aspects need to be added and incorporated into the NC3A systems.

6.4.2. Risk Communication and Management

Description: Communication of the characteristics of a pandemic disease prior to its initial release is the first stage in the management of the consequences. Guidance should be provided on how,

why, where, when and to whom information should be made available. The level of information should be tailored to the target audience and will require an understanding of variables, such as cultural differences, language and educational attainment. The nature and role of the medium in which the information is transferred and the frequency of its delivery will need to be understood. Following the event, normal infrastructure mechanisms may be unavailable and so an understanding will be required as to how new messages can be transmitted through a damaged infrastructure to inform the population of the state of the pandemic as well as the state of the services that have been disabled by the event.

Purpose: Any research proposal will require international collaboration across military and civilian organizations. Risk management and simulation tools will be required to help consequence management continuously monitor and assess the extent and scope of the disease spread and whether progress is being made to recovery. Communication about the spreading of the disease will give valuable information to the terrorists, and mostly generate panic. Need to address to what extent will we be obliged to deliver to the public the real information, and if we can find general public procedures which do not require identification of the nature of the agent.

6.5. MODELLING & SIMULATION

6.5.1. CT Performance and Assessment Models

Description: To gain some insights into the capabilities and limitations of CT Indications & Warning mechanisms and tools, prior to the development of real applications. This can include modelling infrastructure vulnerabilities and the consequences of their attack.

Purpose: To develop modelling that allows NATO to assess threat and quality of indications and warnings. This is similar in concept to the current NATO Indicator and Warning system, which is managed by NATO IMS. This approach will use the results of previous proposals.

6.5.2. Modelling and Simulation

Description: System models can be used to simulate attacks and determine vulnerabilities.

Purpose: To develop computerized representations of systems to model the way they are built and simulate their behaviors. The computer code is used to design the system, assist its performance and train the staff operating them. The models can be relatively coarse or very detailed.

6.5.3. Urban Dispersion Modelling

Description: Modelling and simulation techniques can be used to assess urban dispersion of biological agents.

Purpose: To develop modelling and simulation techniques for the spread and propagation of biological agents in an urban environment. This includes, e.g., flow-field modelling. Important considerations include understanding dispersion mechanisms so as to derive better protection measures.

6.5.4. Epidemiological Modelling

Description: Modelling can be used to portray epidemiological effects.

Purpose: To model the spread of disease in a population as a function of social and behavioral aspects. Identify variables and dependent factors. An extensive list of diseases needs to be considered.

6.6. BIOLOGICAL

6.6.1. Cooperation on Decontamination Technology

Description: Our capability in decontamination in general is not good. Radiological decontamination is particularly difficult and no really effective means exists for accomplishing the task. For a radiological attack against the environment, we could say that the task is virtually impossible. Challenges are also present in the decontamination of biological and chemical agent.

Purpose: A research program across the area of decontamination would be very helpful.
Special areas of difficulty are mustard, spores. It remains difficult to decontaminate severely wounded patients.
Decontamination technology across the CBRN domain is primitive and "rendered safe verification" technology is largely non-existent or primitive (e.g., swipes with blood agar assays for anthrax contamination). This cooperative effort would focus on the hard problems of the chemistry of decontaminating "stuff" in all different environments. Two hard problems: mustard agent and mixed radiation contamination. (HFM Panel)

6.6.2. Medical Treatment Modalities for Consequence Management of Chemical, Biological, Radiological and Nuclear Events

Description: Research and development is required to produce antiviral/bacterial etc. substances that can be used in both a prophylactic capacity and/or treatment role for both humans and animals.

Purpose: Is there a need to re examine the NATO agents' priority list? This could be a question to put forward at the WMDC coordinated workshop in Cologne. If so then this task could go to the Biomedical working group under the NATO Standardization Agency.
Because of the increasing number of emerging bio-warfare pathogen threats (e.g., infectious diseases and genetically modified agents) there is a need to develop generic, or "multi purpose" vaccines (e.g., immune modulators).
How do we ensure that the health and defence authorities work closely together on this particular challenge?
National medical doctrines differ already on pre vs. post treatment of agents. Side effects must be addressed also.
The hard problems here are:

- Anti-virals (but if successful provides significantly wider prospects of treatment for unknown pathogens)
- Chem. agent (e.g., inhaled mustard treatment)
- Radiation doses sufficient to progress to peritoneal sepsis

6.7. ACCESS CONTROL

6.7.1. Stricter Control of Small Aircraft

Description: Modern aircraft can be flown and landed remotely.

Purpose: Propose to incorporate into new aircraft remote controls that can disable on-board controls in the event of a hostile take-over. The cost and complexity is high; however, there are potential non-terrorist opportunities for use as well. It is difficult to retrofit existing aircraft.

6.8. TRAINING

6.8.1. Novel Techniques and Technologies for Training First Responders and Higher Echelons

Description: There is a requirement to investigate; the generation of, the compatibility of standards for, and identify the specific authorities in NATO Nations for undertaking, training via distance learning for "first responders" and medical practitioners.

Computer-based training (also termed asynchronous learning or advanced distributed learning) offers an Internet based modality that has a reasonable probability of building broad knowledge and an operationally useful Consequence Management (CM) response capability across the echelons of persons who will engage in CM (i.e., from the national leaders to CM professionals to community citizen teams). (HFM Panel)

Purpose: A coordinated and cooperative approach should be instigated to build the essential cognitive science foundation and the techniques/standards for verifying and validating computer-based learning modules for CM.

Simulations and simulation tools need to be examined, and where lacking, improved and developed to support this type of training, and to add more realism and realistic effects to the training process.

6.9. MATERIAL TAGGING

6.9.1. Tagging

Description: Raw materials can be used as weapons including bombs, biological or chemical agents, etc. Attaching overt or covert markers to raw material or containers of raw materials entering in the fabrication of explosives and weapons could be a solution. These markers would be chosen to be easy to detect by surveillance systems deployed to protect high-value targets. As an example, a specific molecule could be attached to fertilizing material often used to fabricate amateur bombs. Also an electronic tag could be attached to the bags containing high explosives to track their movement.

Purpose: It is proposed to study the following topics:

- Chemical tagging of raw material read out by:
  - Nuclear Quadratic Resonance;
  - Laser fluorescence, absorption or transmission;
  - Spectroscopy; and
  - Potentially others
- Radio Frequency (RF) tagging of the packaging read out by an active or passive mean;
- Markings or naturally existing tags i.e. pattern recognition (signs, pictures, shapes, eyes, face, fingerprints, picture, etc.).

6.10. WEAPONS

6.10.1. Novel Energetic Materials

Description: As evidenced by the practices of the Al Queda and Taliban leadership in Afghanistan, terrorists will seek refuge in underground bunkers, caves, tunnels and other facilities that are perceived to be sanctuaries from NATO offensive capabilities. Our ability to deny sanctuary to terrorists is key to ensure a robust counter-action strategy. The development of more energetic materials, whose energy release is tuned to the exploitable vulnerabilities of underground sanctuaries, is an essential element of such a capability. The benefit of higher-energy density explosives are realized in terms in increases in weapon lethality, weapon range, and platform load-out. Novel energetic materials offer the ability to tailor pressure, impulse and temperature profiles to optimally match target response characteristics.

Purpose: Near-term research should focus on "designer molecules", such as cubanes and high-nitrogen content molecules. Longer-term research should include research materials exhibiting high-energy meta-stable states as well as other more exotic, higher risk, high payoff technologies. Issues related to military utility and producability should also be addressed.

6.10.2. Special Payloads to Defeat CBRN Threats With Minimum Collateral Damage

Description: Terrorist threats encompass a broad spectrum of agents and explosives that could be used to create mass casualties.

Purpose: NATO must have an equally broad spectrum of special payloads, both man-portable and platform-delivered, capable of neutralizing such materials, in storage or in transit, without posing significant collateral hazards to civilian populations or the environment. Payloads of interest would include, for example, incendiary devices to neutralize chemical and biological agents, bacteriophage agents that consume bacteria or virus material; and special explosive devices to defeat improvised nuclear devices.

6.11. PHYSICAL PROTECTION

6.11.1. Personal Protective Equipment

Description: Personal protective equipment can be enhanced from an anti-terror perspective since a typical terrorism scenario would differ from traditional crisis management and warfighting scenarios.

Purpose: : To provide garments, breathing apparatus, masks, etc., to protect personnel that are easy to put on and use, while not impacting workload in a significant manner. Such equipment must protect against a wide range of potential pathogens, including those that might be created by genetic engineering and other technologies. The "operational life" of this equipment, under a terrorist scenario, might be shorter for first line emergency units since they will normally need only a few hours of endurance for their protective equipment compared to that required for longer term sustained military operations under CB conditions. This may result in different total protection system solutions, involving different technical solutions . The basic technologies involved may not , however, be different. The most important difference lies at the system concept level. The key to good solutions for anti-terrorist purposes is to develop systems that do the job with a minimum of operational limitation at minimum cost.

6.11.2. Hardening Constructions

Description and Purpose: Hardening constructions against blast, fragments and fire with the aim that it can withstand an explosion in such a way that:

- The remaining structure/construction does not fall apart;
- The collateral damage from the breaking of glass windows is kept at the lowest level;
- The fire going along with the blast is addressed in the design by using fire resistant materials and devices.

6.11.3. Shock-wave Mitigation Devices

Description: Mitigation is the reduction of the effects of an explosion, especially blast propagation and effects, but also fragments and fire.

Purpose: The objective is to:

- Keep the propagation of the blast wave inside the building to a low level, e.g. using blast resistant doors;
- Locate blast-screens (which can absorb or deflect the blast wave) in adequate spots in order to protect the building and its occupants;
- Design the building to avoid focusing of the blast;
- Minimize fire spreading by means of fast fire suppression.

6.11.4. Evacuation Aid

Description and Purpose: Study possible improvements of procedures or devices (including emergency exits) in order to accelerate evacuation of a large amount of people from buildings.

7. NON-TECHNICAL CONSIDERATIONS

During the process of developing technology ideas for combating terrorism, many non-technical factors of great importance became apparent, and are listed here.

7.1. Data Protection

Database linking and sharing will face several non-technical issues that should be addressed in parallel with technology development (although development of this capability should not be delayed due to potential non-technical issues):

7.1.1. National Sensitivities

Optimized database linking and sharing will require multi-national access to a potentially wide range of security, social and economic information about populations of both Alliance and non-Alliance countries. States are likely to differ in their willingness to make this information available, introducing non-uniformity and partial coverage. Potential solutions include encryption of personal identifiers to ensure anonymity of individuals.

7.1.2. Legal Limitations

In addition to issues associated with sensitivities over the sharing of personal data, there may be difficulties due to the differing legal systems in NATO member states over issues such as the sharing and transmission of personal data. Further study, including liaison with law enforcement agencies, would indicate the extent to which this is likely to be an issue that may need to be addressed (possibly requiring legislative action).
In addition to the sensitivities associated with the sharing of personal data, there may be issues associated with differing national legal systems over issues such as the protection of personal data. Further study, including liaison with the law enforcement community, may indicate the extent to which legislative action may be required to enable database sharing.

7.1.3. Sharing Existing Technologies

Many existing technologies exist for data mining and exploitation. Initial work may include the sharing of this existing work and their use on trial data sets.

7.1.4. Sharing Lessons Learned

A mechanism to share lessons learned during the development of data sharing would be highly beneficial, based on the existing NATO mechanisms for sharing operational lessons.

7.2. Military & Non-Military Coordination

- Harmonizing of doctrine and requirements between military & non-military entities is necessary because responding to a terrorist event involves both entities. Agreeing or at least understanding how each will respond will prevent delays in responding to an event.

- Simulation-based gaming can be used to test a combined response between military and civil authorities. This will help them refine policy and establish necessary links to assure an effective response with efficient sharing of responsibilities

7.3. Combating a Medical Pandemic Presents an Array of Non-Technical Concerns

- Acceptability of global vaccination
- Cross-departmental problems and organization
- Funding and resources
- Storage or supply of vaccines and medication
- Linking with non-NATO information systems
- Sensitivities of connecting databases

7.4. Need for Modelling and Simulation Support

Much of the RTO work on CT will benefit significantly from being based on a broad range of terrorist attack scenarios. This is important both as a basis for operations/systems analysis, for establishing requirements and priorities, and for guiding the research and development of specific situations. It is, therefore, very important to identify, specify, and characterize a broad spectrum of scenarios relevant for research and development in the area of combating terrorism modelling and simulation efforts.

7.5. More Rapid Process to Identify Capability Needs and Translate them into R&T

There is a requirement to identify a process within NATO for more rapidly identifying capability needs and requirements and then to develop a methodology for rapid translation and implementation into R&T programs. Possible mechanisms to be examined for implementing this process are Workshops and Brainstorming Sessions (Similar to the NATO RTA Combating Terrorism Workshop).

7.6. Better Method of Using Lessons Learned

There is a great deal of existing National data on Lessons Noted/Learned from Combating Terrorist activities. It is proposed that a survey be undertaken of this data, its format and releaseability, and then to examine the possibility of integrating and analyzing the data into a NATO Lessons Learned Center. The possible use of integrating the expertise and experience resident within the NATO RTA and the NATO Joint Analysis and Lessons Learned Center (JALLC) should be examined.

7.7. Increase use of Advanced Concept Technology Demonstrator Programs (ACTDs), Experimentation within R&T to Facilitate Feedback from Military to R&T Community

It is proposed that the use of existing Advanced Concept Technology Demonstration Programs (ACTDs) within R&T be examined to provide a more rapid feedback of Military operational considerations and requirements to the R&T community.

8. WAY-AHEAD

This report contains ideas and suggestions for work, research, studies and analysis which might be undertaken in order to better combat terrorism. It was produced through intense but short consideration of the possibilities by a group of about 70 NATO and national experts. The recommendations are brief and necessarily lacking in detail.

Use of these recommendations is seen as lying in three areas:

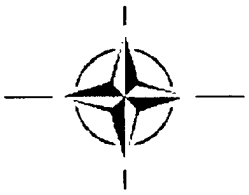
8.1. The report will be distributed throughout the nations of the Alliance. They are expected to distribute it within their R&T communities for consideration by national experts as to whether the ideas and suggestions are suitable for the definition of a national program, based on one or more of them. A related benefit of the workshop is that national representatives who participated are expected to carry home with them the ideas that were discussed (even those that were not documented fully) and to expand these ideas in a national context.

8.2. The report will be distributed to each of the panels of the RTO and to the NMSG. These bodies are charged with considering the issues and studies recommended in it and to define how they might contribute to them, either individually as panels or jointly. They will be asked to report back to the RTB on their conclusions and recommended way ahead.

8.3. As the report is reviewed by national experts, it is expected that additional suggestions for areas of study will come to light. The RTO would like to encourage continued dialogue and requests that comments and recommendations be forwarded to the RTA through respective National Coordinators.

APPENDICES

APPENDIX 1. Detailed Agenda



NATO RTO Combating Terrorism Workshop

5-7 February 2002

Tuesday, 5 February 2002

Attire: Military – Uniform Of the Day (UOD), Civilian – Business Attire

0715 **Guests Arrive at Anteon Corporation**
1560 Wilson Blvd.
Suite 400 (4th floor)
Arlington, VA

0715-0800 **Registration**

0800-0820 **Welcome and Introduction**

Welcome & Introduction
Mr. Nils Holme (NO)
Chairman, Research and Technology Board, NATO

Welcome
Dr. Don Daniel (US)
Deputy Assistant Secretary of the Air Force (Science, Technology and Engineering)

Introduction of Facilitatators
Mr. Jim Mattice
Universal Technology Corporation
Lead Facilitator, NATO/RTO Combating Terrorism Workshop

Context-Setting Session

0820-0935 **Context-Setting Speakers**

NATO Terrorist Threat Assessment
LtCol Philip Stack (UK)
Terrorist Intelligence Section
International Military Staff Intelligence Division
NATO Headquarters, Brussels BE

Catastrophic Terrorism and Asymmetric Warfare: a deadly cocktail
Major-General Franklin E. van Kappen, Marine Corp, retired (NL)
former Military Adviser to the Secretary General of the U.N.

Arturo Relanzàn Sanchez-Gabriel (SP)
Chief of Operations, Operational Support Division
Centro Superior de Informacion de la Defensa, MOD

0935-1000 **Morning Break**

1000-1130 **Context-Setting Speakers (continued)**

Professor Sir Keith O'Nions FRS (UK)
Chief Scientific Adviser Ministry of Defence

Dr Ron Sega (US)
Director Defense Research and Engineering
Director, DoD Combating Terrorism Technology Task Force

Dr Penrose (Parney) Albright (US)
Assistant Director for National Security and Homeland Defense
Office of Science and Technology Policy
Executive Office of the President

1130-1200 **Panel of Morning Context-Setting Speakers**
All attendees are welcome to ask general questions to the panel or specific questions to one of the morning speakers.

1200-1245 **Lunch**
Catered Lunch

1245-1445 **Context-Setting Speakers (continued)**

Mr. Michael S. Markin (UK)
Director General (Research and Technology) Ministry of Defence (HQ)

The Canadian CBRN Research and Technology Initiative:A Holistic Approach to Counter-Terrorism S&T
Dr. John Leggat (CA)
Assistant Deputy Minister Science & Technology, and CEO Defence R&D

Overview of the Technical Support Working Group Process
Mr Edward J. McCallum (US)
Office of the Secretary of Defense, Director of Combating Terrorism Technical Support Office

DARPA's Technology Projects to Combat Terrorism
Dr. Jane Alexander (US)
Deputy Director of the Defense Advanced Research Projects Agency (DARPA)

1445-1515 **Afternoon Break**

1515-1605 **Context-Setting Speakers (continued)**

An Integrated Approach for Developing the Analytical Framework of Combating Terrorism
Dr Barbarosoglu (TU)
Director, CENDIM Center for Disaster Management, Bogazici University

RTO Contribution to Combating Terrorism
Mr. Kenneth A. Peebles (CA)
Director, NATO Research and Technology Agency

1605-1630 **Panel of Afternoon Context-Setting Speakers**
All attendees are welcome to ask general questions to the panel or specific questions to one of the afternoon speakers.

Plenary Session I

1630-1730 **Facilitated Review of Context**

Workshop Goals
Mr. Nils Holme (NO)
Chairman, Research and Technology Board, NATO

Facilitation Approach
Mr. Jim Mattice
Universal Technology Corporation
Lead Facilitator, NATO/RTO Combating Terrorism Workshop

1730-1800 **Proceed to Arlington Hyatt**

Poster Session

1800-2000 **Poster Session and Evening Social**
Arlington Hyatt, Senate Ballroom

Wednesday 6 February 2002

Attire: Military – UOD, Civilian – Business Attire

0800 **Guests Arrive Anteon Corporation**
1560 Wilson Blvd.
Suite 400 (4th floor)
Arlington, VA

0800-0830 **Registration**
Suite 400

0830-1200 **Concurrent Facilitated Workgroup Sessions**
Participants have been pre-assigned to one of the following Workgroups
-- *Indications and warnings*
-- *Survivability and denial*
-- *Consequence management and recovery*
-- *Attribution and Counter-Action*

1200-1330 **Lunch**
Attendees are free to enjoy lunch in the Rosslyn area. A list of nearby restaurants is available.

1330-1530 **Concurrent Facilitated Workgroup Sessions (continued)**

1530-1700 **Workgroups Prepare Report of Progress, Issues and Opportunities**

1700-1900 **Proceed to Arlington Hyatt**
Personal time

1900-2200 **Hosted Dinner with Guest Speaker**
Arlington Hyatt
Senate Ballroom

Forging a Transatlantic Strategy for Terrorism and Asymmetric Warfare
Mr. Anthony H. Cordesman (US)
Arleigh Burke Chair and
Senior Fellow, Strategic Assessment
The Center for Strategic and International Studies
Washington, DC

Thursday, 7 February 2002

Attire: Military – UOD, Civilian – Business Attire

0800 **Guests Arrive Anteon Corporation**
1560 Wilson Blvd.
Suite 400
Arlington. VA

0800-0830 **Registration**
Suite 400

Plenary Session II

0830-0930 **Workgroup Presentations**
A representative from each of the four workgroups will give a 20-minute overview of the results of the brainstorming and discussions from the previous day.

0930-1000 **Context-Setting Speaker**

Ambassador Francis Taylor (US)
Ambassador at Large and Coordinator for Counterterrorism
US State Department

1000-1030 **Morning Break**

1030-1050 **Workgroup Presentations (continued)**

1050-1200 **Review of Workgroup Results**
Facilitation Team
Plenary discussion of workgroup results, and selection of topics for further refinement and development.

1200-1330 **Lunch**
Attendees are free to enjoy lunch in the Rosslyn area. A list of nearby restaurants is available.

1330-1500 **Final Facilitated Workgroup Sessions**
Based on Plenary Session feedback, each workgroup will finalize lists of Combating Terrorism technology areas and build the initial framework for RTO Technical Activity Proposals (TAPs).

1500-1520 **Afternoon Break**

Plenary Session III

1520-1600 **Workgroup Presentations**
A representative from each of the four workgroups will give a 10-minute overview of their respective final workgroup session.

1600-1630 **Facilitator Summary of Workshop Results, Way Ahead**
Mr. Jim Mattice
Universal Technology Corporation
Lead Facilitator, NATO/RTO Combating Terrorism Workshop

1630-1700 **Closing Remarks**
Mr. Nils Holme (NO)
Chairman, Research and Technology Board, NATO

APPENDIX 2. Attendee List

Mr Johan Aas, NO, SAS Panel
Dr Penrose Albright, US, White House Office of S&T
Prof Dr Nafiz Alemdaroglu, TU, SCI Panel Chairman
Dr Jane Alexander, US, DARPA
Mr Todd Anderson, US, Project Manager, CTTSO
Dr Robert Angus, CA, HFM Vice-Panel Chairman
Mr Gary Appleton, US, RTA Assistant Director
LTC Norman Atkins, NE, SHAPE
Mr Frederick Baedke, US, Workshop Facilitator
Prof Dr Gulay Barbarosoglu, TU, Bogazici University
Dr William Berry, US,
Ms Ann Bradfield, CA, SAS Panel
Mr Graham Burrows, UK, NMSG Executive
Dr Rudolf Buser, US, SET Panel
LTC Scott Campbell, US, SCI Executive
Mr Paul Chatelier, US
COL Patrice Claveau, FR, SAS Panel
Dr Graham Coleman, UK, AVT Panel
Dr Peter Colins, UK, RTB Member
Mr Frederico Colas Rubio, SP
Ms Victoria Cox, US, US National Coordinator
Dr-ING Luigi Crovella, IT, SCI Panel
Dr Judith Daly, US, OSD-ATL
Dr Don Daniel, US, RTB Member
Mr Jeffrey David, US, Deputy Director CTTSO
Mr Gary DuBro, US, Workshop Facilitator
ICA Alain Dunaud, FR, NMSG Member
Dr Denis Faubert, CA, SET Vice-Panel Chairman
Dr Robert Foster, US, HFM Panel
Mr Raymond Herrera, US, Admin Support
Dr Daniel Hoffmans, NE, AVT Panel
Dr Myron Holinko, US
Mr Nils Holme, NO, RTB Chairman
Ms J.R. Holt, US, Workshop Facilitator
Dr Anthony Hyder, US, SET Panel
SSGT Patricia James, US, RTA Security
Dr Anna Johnson-Winegar, US, OSD/AT&L
Dr Yolanda Jones King, US, Workshop Co-Organizer and SET Panel
Mr Robert Kean, US, NMSG Member
Ms Kim Kelly, US, Admin Support
Dr John Leggat, CA, RTB Member
Mr Guillermo Leira Rey, SP, NATO Defense Support
Mr Viggo Lemche, DE, SAS Panel
Mr John Lesko, US, Workshop Facilitator
Mr Mike Markin, UK, RTB Member
Ms JoAnne Marsden, UK, HFM Panel

Dr Stephen Martin, US, SNL
Mr James Mattice, US, Workshop Facilitator
Mr Edward McCallum, US, Director, CTTSO
Mr Timothy McClees, US, Office of National Coordinator
Dr Richard McClelland, US, AVT Panel
Dr Ann Miller, US, IST Panel
Dr Fenner Milton, US, SET Panel
Mr Allen Murashige, US, Workshop Co-Organizer and SAS Panel
Col Andrezej Jajgebauer, PL, NMSG Member
Prof Gian Paolo Noja, IT, HFM Panel Member
Sir Keith O'Nions, UK, Chief. Scientific Advisor, MOD
Dr David Oxenham, UK, SAS Panel
Mr John Parmentola
Mr Bharatkumar Patel, UK, SCI Panel
Mr Jeffrey Paul, US, OSD/AT&L
Mr Kenneth Peebles, CA, RTA Director
MGEN Marc Pirou, FR, RTA Deputy Director
Mr Arturo Relanzon Sanchez-Gabriel, SP
Dr Gert Retzer, GE, NC3A
Mr Michael Rugienius, US, DMSO
Prof Emile Schweicher, BE, SET Panel
Mr Ron Sega, US, OSD/DDR&E
LTC Philippe Soete, FR, RTA Deputy SPD
Mr Ragnvald Solstrand, NO, SAS Panel
COL Adam Sowa, PL, NATO IMS
LTC Philip Stack, UK, NATO IMS
Mr Frederick Stahl, US, Workshop Facilitator
Prof Dr Maurus Tacke, GE, SET Panel
Ambassador Francis Taylor, US, State Department
COL Wilhelmus Tielemans, NE, HFM Panel Chairman
Mr Didier Tournemeine, FR, AVT Panel
Dr George Ullrich, US, OSD/AT&L
Mr Dennis van Derlaske, US
Dr Ernst van Hoek, NE, RTB Member
GEN Franklin van Kappen, NE, TNO
Dr Malcolm Vant, CA, IST Panel Chairman
Dr Jacques Vermorel, FR, Head, TSCO
LTC David Weisz, US, RTA Exec Officer, OCD
Dr Ian White, UK, IST Panel
Mr Gerardus Willemsen, NE, SCI Panel
CMDR Brian Williams, US, SACLANTCEN
Mr Colin Wright, UK, SACLANT
Mr Gary Yonke, US, Workshop Facilitator

APPENDIX 3. Poster Session information

Display No.	Title	Presentor
1	General Overview of Belgian Potential Contributions	*Schweicher*
2	3-D Face Recognition	*Beumier*
3	Semi Automatic Help for Aerial Region Analysis	*Schweicher*
4	TeraScreen: Electronic Terahertz Spectroscopic Imaging For Screening Bioweapons and Explosives	*van der Weide*
5	Steganography: Art & Science of Hidden Communication	*Wachter*
6	IST Contributions to Combating Terrorism	*Miller*
7	Fourier Transform Hyperspectral Imager (FTHSI)	*Jones King*
8	Pathfinder and Advanced Distributed Learning	*Schwan, Burrows*
9	NATO Distributed Mission Training	*Schwan, Burrows*
10	Course of Action Tools	*Burrows*
11	Joint Conflict & Tactical Simulation	*Kean*
12	Explosives Detection by Nuclear Quadrupole Resonance	*Garroway*
13	C41SR Technologies for Combating Terrorism Deterrence & Survivability	*Irwin*
14	C41SR Technologies for Combating Terrorism Consequence Management and Recovery	*Fillian*
15	Mobile Back Scatter Imaging by X-Ray	*DuBravac*
16	LIDAR Collection	*Jones, Hardaway*
17	Agent Based Simulation Technology for Counter Terrorist Intelligence	*Waltz*
18	Technology Innovations for Countering Terrorism	*Faubert*
19	Rapid Syndrome Validation Project	*Zelicoff*
20	Handheld Explosives Preconcentrators	*Martin, Baumann*
21	Joint Antiterrorism/Force Protection (JAT/FP) Program	*Hampton*
22	Terrorist Threat Protection	*Mosher*
23	DREO Lab Contributions to National Security Issues	*Vant*
24	Use of Genetic Immunization to Protect Against Anthrax	*Galloway*
25	Integrated Panoramic Night Vision Goggle	*Craig*
26	Agile Vaccines Against Biowarfare & Genetically Modified Agents	*Campbell*
27	Associating & Understanding Information Across Sensors & Message Domains	*Perlovsky*
28	Multiple Topics	*Hoffmans*
29	Social and Psychological Consequences of Chemical, Biological and Radiological Terrorism	*Marsden*
30	Personnel Protection	*Coleman*
31	Situational Awareness Counter Terrorism for the Carriers	*Buss*

APPENDIX 4. Participants Handbook

COMBATING TERRORISM

A Participants' Background Guide for the February 2002 NATO RTO Workshop

INTRODUCTION

This workshop has two equally important goals. One goal is to develop a list of high impact research and technology activities which the RTO can sponsor as part of NATO's overall effort to combat terrorism. A second goal is the multi-national exchange of ideas which will enhance both individual and multi-national research and technology activities for combating terrorism. It is important to strive for a balanced contribution of technologies from the NATO participants. It is also important for facilitators to understand the military mission and functional capability implications of combating terrorism in order to help focus deliberations on technology solutions that evolve. The classical acquisition strategy for combat materiel has put much more emphasis on *requirements pull* than *technology push.* This endeavor will strive to assess the technology efforts that can be capitalized on in support of combating terrorism. For this reason and given the precedent-breaking developments of September 11, 2001 and shortly thereafter, a balanced approach of requirements pull and technology push is deemed appropriate.

Combating Terrorism

Terrorist activity worldwide during the second half of the 20th century and into the first decade of the 21st has shown no sign of abating. Its forms have been evolving and the magnitude of the World Trade Center incident of 2001 clearly displays the potential for the increasing destructiveness of individual events. With the availability of better technologies on the world market, be they obtained overtly (such as communications or information processing) or covertly, the potential exists for either more sophisticated attacks or greater sophistication in the planning of simpler attacks to occur.

Combating Terrorism is the capability to oppose terrorism throughout the threat spectrum, including *antiterrorism* (defensive measures to reduce vulnerability) and *counter-terrorism* (offensive measures to prevent, deter, and respond effectively to terrorist acts). This capability includes personnel protection, tactical operations, explosives detection and defeat, investigative science and forensics, physical security and infrastructure protection, surveillance and collection, detection, monitoring and tracking, intelligence, logistics, communications and training.

MISSION REQUIREMENTS

Operational Capabilities

Key operational capabilities for combating terrorism can be incorporated into three principal categories: *prevention, protection and response.* These operational capabilities further delineate the categories and reflect distinctly different facets of the problem, and each offers its own set of challenges

and opportunities. Within these categories specific subelements important to Combating Terrorism on many different fronts have been identified. These will be discussed within each operational capability category.

PREVENTION

The safety and security of military and civilian personnel potentially subject to terrorist attacks can be enhanced by developing new capabilities pertinent to preventing their occurrence. More effective prevention requires the employment of new or improved capabilities for identifying terrorist organizations and monitoring their activities, identifying and tracking individual terrorists, detecting and restricting access to a wide range of potential threat agents and explosive devices, limiting access to areas of significant potential vulnerability, and, when necessary, conducting decisive preemptive strikes. All of these capabilities are strongly interrelated.

Indications and Warning- Improved terrorist identification, surveillance and tracking capabilities are needed to help prevent terrorist acts by facilitating the timely interdiction of terrorists and threat agents and devices; early warning of impending attack will also enable the implementation of protective countermeasures. Enhanced capabilities for detecting threat agents and devices at extended standoff distances will strengthen perimeter security and increase warning time, again facilitating countermeasure actions. Such actions will also be enhanced by the development of personnel alerting systems.

Deterrence- Improved capabilities for detecting terrorists and threat agents and devices to enable more effective entry-point screening and improved perimeter security, which will help to deter types of attacks by terrorists. Terrorist awareness of significant preemptive strike or counter action capabilities can also be expected to provide deterrence benefits.

Denial- Denying access to potential targets is a critical aspect of preventing terrorist attacks. Effective means for limiting access to facilities, combined with advanced threat detection and screening capabilities will inhibit many actions by terrorists by preventing them from reaching intended targets.

Preemptive Strike- Under some circumstances, where the potential consequences of anticipated terrorist attacks are great, the execution of rapid and precise preemptive strike operations may offer the only assured means for preventing their occurrence.

PROTECTION

Although improved capabilities for preventing terrorist actions will help to reduce the overall threat, preventing all such incidents cannot be guaranteed. Advanced supplemental protective capabilities for combating terrorism that help to limit the effectiveness and mitigate the consequences of terrorist attacks on facilities, elements of each country's defense infrastructure and personnel are needed.

Facilities- New building design features and new means for mitigating the effects of explosive blasts are needed to reduce the consequences of terrorist attacks on a variety of military and other government facilities. Improved capabilities for entry-point screening of personnel, automobiles and cargo vehicles will also contribute to the protection of facilities.

Infrastructure- Advanced capabilities for protecting critical elements of the defense and civilian infrastructure including communications networks, transportation systems, electric power grids, natural

gas and petroleum distribution systems, food and water supply systems and health and sanitary systems are required. The degree to which some of these systems are shared by military and civilian users may vary among member nations.

Personnel- The protection of military and civilian personnel against terrorist attacks will be enhanced through advanced building design features, new structural blast mitigation systems, advanced body armor and improved chemical/biological (CB) agent protection systems. Improved capabilities for detecting, neutralizing and limiting the dissemination of chemical and biological agents are also needed to enhance personnel protection.

RESPONSE

A comprehensive range of capabilities is required for responding to terrorist attacks. These capabilities address recognized needs pertinent to crisis management, effective and expeditious handling of the consequences of various types of attack, identifying the perpetrators of terrorist actions, and planning and executing appropriate retaliatory operations.

Crisis Management- The availability of improved capabilities for detecting, diagnosing and disabling terrorist threat devices, including small improvised explosive devices (IED's), large vehicle bombs, and CB agents will help to reduce the severity of many attacks. Effective procedures for preventing the release and dissemination of CB threat agents are also needed.

Consequence Management- New capabilities for countering and effectively handling mass casualties and mass decontamination of military and dependent personnel, including injuries caused by explosives or associated with the release of chemical and biological agents are required. Improved measures for responding to the effects of attacks on elements of the defense infrastructure that will minimize their impact and enable rapid restoration of compromised services are also needed.

Attribution and Counter Action- The development of improved capabilities for rapidly and reliably identifying the perpetrators of terrorist incidents will enable the planning and execution of appropriate counter-action operations as well as the implementation of effective countermeasures to possible additional attacks. Improved forensic capabilities will also support criminal prosecution efforts by the appropriate governmental entities in each country. The ability to execute a variety of military operations in response to terrorist attacks is important for deterring future incidents. New capabilities for conducting such operations with greater speed, precision and a higher level of assured effectiveness are needed to reduce casualties suffered by national/coalition forces and to minimize fratricide problems, particularly in hostage situations.

FUNCTIONAL CAPABILITES

To achieve the operational capabilities as described above the following functional capabilities for military operations in support of combating terrorism have been defined. These are intended to serve as a catalyst for deliberation in the workshop and may be modified as a result of that process.

Threat Device Detection- the ability to use portable detection equipment to accurately, automatically and safely detect threat chemical, biological, radiological, nuclear and explosive devices from remote locations.

Terrorist Surveillance and Tracking- the ability to observe, identify and track threat targets from remote locations, at any time of the day or night, and under adverse weather conditions.

Situational Awareness- the ability to rapidly access, fuse and visualize information from multiple databases to evaluate and assess operational environments.

Precision Insertion and Targeting- the ability to precisely acquire and attack terrorist targets while minimizing collateral damage.

Simulation and Training- the ability to effectively use advanced modeling and simulation tools and virtual-reality immersion devices to support realistic training of NATO/national defense personnel in both anti-terrorism and counter- terrorism operations.

Threat Warning Dissemination- the ability to disseminate information throughout the chain of command or line of authority on all terrorist activity identified through all intelligence methods and sources (getting the right threat warning information to the right person in a timely manner).

Chemical/Biological Agent Protection- the ability to protect personnel, equipment and facilities from chemical and biological threats through a combination of samplers, detectors and prophylaxes (including pre-attack treatments or garments).

Threat and Vulnerability Assessment- the ability to effectively use situational awareness information, weapons effects representations and modeling and simulations-based analytical tools in assessing the vulnerability of NATO/national forces, civilian personnel, equipment and structures to terrorist attack.

Protective Materials and Structures- the ability to use protective materials and advanced building design and construction features to protect personnel and facilities subjected to attack by ballistic and explosive means.

Remote Operations- the ability to gather information, take action against a threat device/target, or respond to a terrorist incident from a position that is removed from the immediate area of concern and that may also provide protection, standoff or concealment.

Threat Device Disablement- the ability to use robotics, electromagnetic radiation, water disruption techniques, explosives, kinetic energy, chemicals and other means to safely disable or deactivate threat weapon devices.

Incident Analysis- the ability to quickly and accurately sense and determine the immediate and longer term effects of terrorist attacks.

Mitigation of Chemical/Biological Agents- the ability to quickly and effectively minimize the effects of chemical and biological attacks.

Mass Casualty Medical Care- the ability to quickly locate casualties and provide life-sustaining care to large numbers of victims through all appropriate means, including the use of telemedicine.

Military/Law Enforcement Organization Coordination- as applicable, depending on the location of the activity, the ability to have seamless communications between and among the military entities and between the military and other government ministries/agencies and civilian organizations.

Forensic Analysis- the ability to examine evidence and determine the type, cause, perpetrator(s) or initial location of a terrorist attack using advanced technical means, including chemical and DNA analyses and post-attack simulation and assessment tools.

Post-Incident Recovery- the ability to quickly recover from a terrorist attack and return to a protective posture.

WORKSHOP TAXONOMY

In planning for the execution of the workshop, a structure was adopted which aggregated key sub-elements of the mission operational capabilities into four working areas:

- Indications and Warning
- Survivability and Denial
- Attribution and Counter Action
- Consequence Management and Recovery.

The rationale for this was based on the need to have a manageable number of working groups, each with a coherent thrust comprised of related sub-element areas. Additionally, this same taxonomy was adopted from a U.S. DDR&E Combating Terrorism Task Force which has been established to evaluate applicable technologies in the US DoD domain. Note that not all sub-elements were included and one, Recovery, was added, being a natural outgrowth of Consequence Management.

The utilization of this taxonomy along with the functional capabilities can assist to guide the selection and assessment of technologies appropriate to these functional capabilities as part of the workshop deliberative process.

REFERENCE:

Joint Warfighting Science and Technology Plan, U.S. Department of Defense, Deputy Under Secretary of Defense (Science and Technology), February 2000.

APPENDIX 5. Facilitation Process

The first day established the context of recent world wide terrorism activities from the perspectives of several NATO organizations and national leaders. Panel discussions of context-setting speakers rounded out the day, along with an evening poster session that represented various national counter-terrorism efforts that might provide a partial basis for future collaboration. The second and third days involved intensive, facilitated concurrent workgroup sessions. It was agreed that political sensitivities, that might at first glance seem too far-reaching, should not interfere with the generation of ideas, i.e. there should be no pre-filtering of ideas. Workgroups named one or more spokespersons to report preliminary progress, and then give a final presentation of areas of potential collaboration.

To facilitate the complicated process of four multi-national groups attacking a very different component of counter-terrorism activity on a severely constrained time line, a full time professional facilitator and common general facilitation process approach was adopted. Workgroups were asked to think about their areas of interest and develop R&T possibilities by examining sequentially:

- possible future terrorist threats
- operational scenarios
- needed capabilities to counter terrorism
- technology deficiencies and possibilities to acquire capability
- research opportunities to address technology deficiencies
- identification of areas of collaboration.

Processes used to focus workgroup activities included:

- consideration of multi-national context perspectives
- continuous preservation of important information
- individual and small group shared experiences from recent terrorist actions in nations
- active consensus building for preliminary and final product reporting.

APPENDIX 6. Table of Abbreviations

ADAP-P3	Alliance Directory Access Protocol-P3
AFOSR	Air Force Office of Scientific Research (US)
ATM	Automatic Teller Machine
AUV	Autonomous Underwater Vehicle
AVT	Applied Vehicle Technology
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (US)
CBRN	Chemical Biological Radiological and Nuclear
COTS	Commercial Off The Shelf
CT	Combating Terrorism
DDR&E	Director, Defense Research and Engineering (US DoD)
GPS	Global Positioning System
HFM	Human Factors and Medicine
IMS	International Military Staff
IST	Information Systems Technology
MOD	Ministry of Defence
NATO	North Atlantic Treaty Organization
NBC	Nuclear, Biological, Chemical
NC3A	NATO Consultation, Command and Control Agency
NMSG	NATO Modelling and Simulation Group
RTO	Research and Technology Organization
RTB	Research and Technology Agency
RTG	RTO Task Group
SAF/AQR	Secretary of the Air Force, Acquisition Research Directorate (US)
SAS	Studies, Analysis and Simulation
SCI	Systems Concepts and Integration
SET	Sensors and Electronics Technology
UAVs	Unmanned Aerospace Vehicles
WMD	Weapons of Mass Destruction